

# Public Quantum Communication and Superactivation

Fernando G.S.L. Brandão and Jonathan Oppenheim

**Abstract**—Is there a meaningful quantum counterpart to public communication? We argue that the symmetric-side channel – which distributes quantum information symmetrically between the receiver and the environment – is a good candidate for a notion of public quantum communication in entanglement distillation and quantum error correction.

This connection is partially motivated by [Brandão and Oppenheim, arXiv:1004.3328], where it was found that if a sender would like to communicate a secret message to a receiver through an insecure quantum channel using a shared quantum state as a key, then the insecure quantum channel is only ever used to simulate a symmetric-side channel, and can always be replaced by it without altering the optimal rate. Here we further show, in complete analogy to the role of public classical communication, that assistance by a symmetric-side channel makes equal the distillable entanglement, the recently-introduced mutual independence, and a generalization of the latter, which quantifies the extent to which one of the parties can perform quantum privacy amplification.

Symmetric-side channels, and the closely related erasure channel, have been recently harnessed to provide examples of superactivation of the quantum channel capacity. Our findings give new insight into this non-additivity of the channel capacity and its relation to quantum privacy. In particular, we show that single-copy superactivation protocols with the erasure channel, which encompasses all examples of non-additivity of the quantum capacity found to date, can be understood as a conversion of mutual independence into distillable entanglement.

## I. INTRODUCTION AND RESULTS

Suppose two trusted parties, Alice and Bob, and a malicious third party, Eve, share noisy classical correlations given by a joint probability distribution  $P_{XYZ}$ . These could come e.g. from measurements on a quantum state shared by them, or from a noisy communication channel, which the eavesdropper is trying to tap. If Alice and Bob's distribution contains some correlations that are partially unknown to Eve, they can exploit this to distill a secret-key (a shared random variable which is arbitrarily close to being perfectly correlated between Alice and Bob, and completely unknown to Eve). This process of obtaining key by previously established correlations is known as *information-theoretic* key agreement [1], [2], [3], [4], alluding to the unconditional security of the protocol guaranteed by information-theoretic considerations, and not conditional on any computational-hardness assumption.

A key resource in this paradigm is *public communication*, which is conveniently represented by a symmetric broadcast

channel which delivers the same information to Bob and Eve (or Alice and Eve, if the communication is coming from Bob). The notion of public communication is useful first because it is a realistic one: in many practical situations the parties have access to an authenticated channel which they might freely use to communicate, but which might nonetheless be subject to eavesdropping. Second, the ability to communicate by a public channel turns out to be instrumental in the development of an elegant, and tractable, theory of secret-key distillation [2], [3], [4].

For example, in the *one-way* or *forward* public communication scenario (which is the one considered throughout the rest of this paper), only Alice is able to send public messages to Bob and Eve. In this case the distillable secret-key rate of the distribution  $P_{XYZ}$  (when the parties are given infinitely many independent realizations of it) is given by [2], [3], [4]

$$C(P_{XYZ}) = \sup_{X \rightarrow V \rightarrow U} I(V : Y|U) - I(V : Z|U), \quad (1)$$

with the conditional mutual information  $I(V : Y|U) := H(VU) + H(YU) - H(VYU) - H(U)$ , the Shannon entropy  $H(X) := -\sum_x P_{X=x} \log P_{X=x}$ , and the supremum taken over the Markov chain  $X \rightarrow V \rightarrow U$ .

The formula in Eq. (1) is so-called *single-letter*, meaning that an optimization over a single copy of the probability distribution gives the asymptotic rate. Moreover it is *additive*, i.e. for two probability distributions  $P_{XYZ}$  and  $Q_{X'Y'Z'}$ ,  $C(P_{XYZ} \otimes Q_{X'Y'Z'}) = C(P_{XYZ}) + C(Q_{X'Y'Z'})$  [2]. We can then say that Eq. (1) completely characterizes how to optimally distill secret-key in the one-way scenario. In contrast, if one instead consider the task of distilling a key from common randomness without any communication, one finds a much more complicated theory, in which even the determination of which probability distributions allow the extraction of key remains an open problem, let alone the derivation of a tractable formula for the distillable secret-key rate.

In quantum information theory, the paradigm described above has two natural analogues, and both have been extensively analysed [5], [6], [7]. The first is to distill a secret-key from a tripartite quantum state  $|\psi_{ABE}\rangle$  shared by Alice, Bob and Eve [7]. Alice and Bob can perform any operation allowed by quantum mechanics on their shares of the state, while (in the one-way setting considered here) Alice can communicate public *classical* messages to Bob and Eve. The second is entanglement distillation [5], in which Alice and Bob wish to distill Einstein-Podolsky-Rosen (EPR) pairs from a shared state  $\psi_{AB}$  by local quantum operations and, again, *classical* communication from Alice to Bob (here too, although not

Fernando Brandão (fgslbrandao@googlemail.com) is at the Physics Department of Universidade Federal de Minas Gerais, Brazil. Jonathan Oppenheim (jono@damtp.cam.ac.uk) is in the Dept. of Applied Mathematics and Theoretical Physics, University of Cambridge. FB is supported by a "Conhecimento Novo" fellowship from Fundação de Amparo a Pesquisa do Estado de Minas Gerais (FAPEMIG). JO is supported by the Royal Society, and NSF grant PHY-0551164 while at KITP, Santa Barbara.

needed, one can consider that an eavesdropper has a purification of  $\psi_{AB}$  i.e. a pure state  $\psi_{ABE}$  such that  $\psi_{AB} = \text{tr}_E \psi_{ABE}$ , and Eve learns all the classical communication that Alice sends to Bob).

In both paradigms, the shared randomness is extended from the original classical probability distribution to a quantum state. The public communication, however, remains the same; even in the quantum case only classical messages can be publicly communicated. A natural question then emerges: is there a meaningful notion of *public quantum communication*?

A first objection to such a notion comes from the fact that quantum information cannot be copied [8], [9] and, hence, it is problematic to consider a procedure which gives the same quantum information to several parties, as in classical public communication. A second objection comes from practical considerations. Both secret-key and entanglement distillation are important operational primitives, and the paradigm of quantum local operations and public classical communication emerges naturally from the resources which are usually available, e.g. in a quantum key-distribution set-up. So if we do not have an interesting setting where a notion of public quantum communication is needed, why bother with such concept? In this paper we show that, at least in the one-way setting, both objections are not well founded, and that there is room for a useful definition of quantum public communication.

#### A. Symmetric-side Channels

In the same way a broadcast channel (which sends the same information to the two receivers) is employed as a model of a classical public communication channel, we will use a quantum *symmetric-side* channel [10] as a model of quantum public communication. This is the channel which maps quantum information symmetrically between the receiver and the environment (see section II for a precise definition).

Note that although both the receiver and the eavesdropper get the same quantum information in the symmetric-side channel, neither of them get the full information originally contained in the sender's state, so there is no cloning of quantum information. Moreover, if the sender prepares, as the input of the symmetric-side channel, a state diagonal in the computational basis, then the channel has the same effect as a classical symmetric broadcast channel. In this way symmetric-side channels can be seen as at least as a natural generalization of public communication to quantum states.

Symmetric-side channels were introduced by Smith, Smolin and Winter [10] with the goal of obtaining a more tractable upper bound on the quantum capacity of quantum channels, defined as the optimal asymptotic rate at which a quantum channel can transmit quantum states faithfully. They analysed how assistance by a symmetric-side channel could improve the quantum channel capacity and the (one-way) distillable entanglement – given by the maximum rate of EPR pairs that can be asymptotically extracted from a quantum state by local operation and classical communication (from Alice to Bob). Remarkably, they found single-letter, additive expressions for both assisted capacities: for a bipartite state  $\psi_{AB}$  with purification  $|\psi_{ABE}\rangle$ , the symmetric-side channel assisted distillable

entanglement (see section II for a formal definition) can be manipulated into the form

$$D_{ss}(\psi_{AB}) = \sup_{A \rightarrow a\alpha} \frac{1}{2} (I(a : B|\alpha) - I(a : E|\alpha)), \quad (2)$$

using entropic identities and with  $I(a : B|\alpha) := S(a\alpha) + S(B\alpha) - S(aB\alpha) - S(\alpha)$  the conditional mutual information,  $S(a) := -\text{tr} \rho_a \log \rho_a$  the von Neumann entropy, and the supremum taken over all channels which maps  $A$  to  $a\alpha$ . This expression is a direct quantum generalization of Eq. (1) and in itself already suggests a formal analogy of distillable entanglement and symmetric-side channels with classical secret-key and public communication.

#### B. An Operational Motivation

For an operational motivation for the view of symmetric-side channels as public quantum communication, we consider the quantum *one-time-pad* problem analysed and solved in [11] (partially employing the techniques we developed in this paper). The setting is as follows. Alice would like to send to Bob secret classical or quantum messages, using an ideal, but insecure, quantum channel which might be intercepted by an eavesdropper, who should not be able to learn anything about the message being sent.

Alice and Bob can make use of the insecure channel for secure communication if they share in addition a *secret-key*. Then using their secret correlations Alice can encode the message in a way that (i) Bob can decode it in the case that Eve does not intercept the states sent down the insecure quantum channel and (ii) Eve cannot distinguish the different messages if she intercepts the sent states. We assume that the key is given by (several copies of) a quantum state  $|\psi_{ABE}\rangle$  shared by Alice, Bob and Eve and the question is to find out what is the optimal rate at which the state can be used to encrypt classical or quantum messages.

This problem was first considered in the noiseless case, in which Alice and Bob share perfect classical key or EPR pairs [12], [13], [14]. In Ref. [15], in turn, Schumacher and Westmoreland analysed the case in which the key shared by Alice and Bob is a mixed bipartite quantum state  $\psi_{AB}$ , which is not correlated with the eavesdropper. Interestingly, they found the optimal rate at which the state can be used as a one-time-pad for classical messages to be given by the quantum mutual information of  $\psi_{AB}$ :  $I(A : B)_\psi = S(A)_\psi + S(B)_\psi - S(AB)_\psi$ .

In [11] we considered the general case, in which Alice and Bob have an arbitrary quantum state, in general correlated with Eve. We found that the optimal rate at which the state can be used as a one-time-pad for quantum information turns out to be given by Eq. (2). It is intriguing that it is the symmetric-side channel assisted distillable entanglement that appears as the optimal rate, even though the problem makes no mention in any way of the symmetric-side channel.

The proof of our result reveals an interesting aspect of this task: the insecure quantum channel is only ever used to simulate a symmetric-side channel, meaning that in the optimal protocol Alice first locally simulates a symmetric-side channel, sends through the insecure channel the output part of

the symmetric-side channel which would go to Bob, and traces out the part that would go to Eve. It thus follows that there is no difference if Alice and Bob are connected by an insecure ideal channel or a symmetric-side channel!

We can therefore consider the quantum one-time-pad as an operational setting where the idea of a symmetric-side channel as public quantum communication naturally appears (though in an indirect manner).

### C. Superactivation of the Channel Capacity

There is another line of investigation in which symmetric-side channels have been shown very useful: in exhibiting examples of non-additivity of the quantum channel capacity [16]. By the no-cloning theorem [8], [9], the symmetric-side channel can be seen to have zero quantum capacity. However, in [16] Smith and Yard noted that a consequence of Eq. (2) and the formula of [6] for the one-way distillable secret-key rate ( $K_{\rightarrow}$ ) is

$$D_{ss}(\psi_{AB}) \geq K_{\rightarrow}(\psi_{AB})/2, \quad (3)$$

for all bipartite states  $\psi_{AB}$ . The equation above is striking because there are examples of states for which the distillable entanglement is zero, but the distillable secret-key is not [17], [18], [7]. In this way, and by considering quantum channels which generate such states, we find an example of two quantum channels (the symmetric-side channel and the other channel which can only produce states with zero distillable entanglement, but some with positive distillable key) each with zero quantum capacity, but whose tensor product has positive quantum capacity. This effect has been termed the *superactivation* of the quantum capacity.

Equation (3) shows a curious property of the symmetric-side channel: it allows the conversion of secret-key into EPR pairs (at half the rate). An interesting question, raised already in [16] and further explored in [19], [20], [21], asks whether there is a more fundamental relation between entanglement and secrecy in the presence of symmetric-side channels. For instance, might the distillable entanglement and distillable secret-key, when assisted by symmetric-side channels, become the same? Although it is rather unlikely that this is the case (see the remark after the proof of Theorem 8), here we will show that a relaxed version of the statement is true. That brings us to the final concept that we will touch in this work.

### D. Mutual Independence

The definition of secret-key consists of two requirements: (i) Alice and Bob systems should be classical, and perfectly correlated and (ii) their state should not be correlated in any way with the eavesdropper. A relaxed and fully quantum definition of private correlations has recently been introduced [22], in which only the second requirement is kept. Then given a bipartite quantum state  $\psi_{AB}$ , the degree of (potentially noisy) private correlations of Alice and Bob, termed *mutual independence* ( $I_{\text{ind}}(\psi_{AB})$ ), is given by (half) the mutual information of a state extracted by Alice and Bob which is product with Eve's state, who is assumed to hold a purifying state for  $\psi_{AB}$ . Their actions are on asymptotically many copies of  $\psi_{AB}$  and

one can consider the mutual independence under different types of operations e.g. by local operations and classical communication.

An operational significance of this new quantity was given in [22]: the sum of quantum communication by Alice and Bob required to send their state to a receiver, in the presence of free entanglement, is given in terms of the mutual independence rate with no classical communication. Given the view of mutual independence as a more relaxed form of private correlations than secret-key, we might ask whether a similar relation as in Eq. (3) holds. We will show that this is indeed the case and that the relation turns out to be actually stronger than with secret-key.

### E. Our Results

Our first contribution is to introduce an even more relaxed notion of private correlations, which we call *weak mutual independence* (see section II). Its definition is almost the same as that of mutual independence, but here we only require that Alice's state is completely decoupled from Eve's. In the setting where no classical communication is allowed, the optimal protocol is just for Alice to split her system in two and trace out one of them, making herself product with Eve and at the same time trying to retain as much mutual information as possible with Bob. We can then see this quantity as a measure of Alice's ability to perform quantum privacy amplification against the eavesdropper.

In section III we derive an entropic capacity formula (alas, a regularized one) for weak mutual independence in the zero and one-way classical communication cases, something that remains an open question for mutual independence. Our formula turns out to be a direct generalization of both the formulae for (one-way) distillable entanglement and distillable secret-key of Devetak and Winter [6].

Our main result, presented in section IV, is the following: when assisted by a symmetric-side channel, the weak mutual independence rate ( $W_{\text{ind},ss}$ ), the mutual independence rate ( $I_{\text{ind},ss}$ ), and the distillable entanglement ( $D_{ss}$ ) become the same, i.e. for every state  $\psi_{AB}$

$$W_{\text{ind},ss}(\psi_{AB}) = I_{\text{ind},ss}(\psi_{AB}) = D_{ss}(\psi_{AB}). \quad (4)$$

We note that an analogous equation holds true classically, if we replace distillable entanglement by distillable secret-key and redefine the two mutual independence rates removing the half factor presented in the quantum case. Indeed, the rate of weak mutual independence which can be attained classically is at least as large as Eq. (2), as one can even get secret-key at this rate. But it also holds that the weak mutual independence rate cannot be larger than Eq. (2). An optimal protocol for weak mutual independence by public communication consists of two steps: Alice first applies a transformation to her random variable (given by  $n$  realizations of the distribution  $P_{XYZ}$ )  $X_n \rightarrow V_n$  obtaining  $V_n$  and then communicate part of it to Bob and Eve, which in turn we can model as an application of a map  $V_n \rightarrow U_n$  and the communication of the random variable  $U_n$ . As the protocol extracts mutual independence, we must have that, asymptotically,  $I(V_n : Z_n U_n) \rightarrow 0$ , since



Alice's final random variable must be decoupled from Eve's. Therefore the weak mutual independence rate is bounded as follows

$$\begin{aligned} \frac{1}{n}I(V_n : Y_n U_n) &\lesssim \frac{1}{n}I(V_n : Y_n U_n) - \frac{1}{n}I(V_n : Z_n U_n) \\ &= \frac{1}{n}I(V_n : Y_n | U_n) - \frac{1}{n}I(V_n : Z_n | U_n) \\ &\leq C(P_{XYZ}), \end{aligned} \quad (5)$$

where the equality in the second line follows from a simple entropic manipulation and the inequality in the last line from the additivity of  $C(P_{XYZ})$ .

Eq. (4) is also key for our result in [11] on the quantum one-time-pad. A protocol for sending classical messages would be to first distill mutual independence using the insecure channel to simulate a symmetric-side channel. One then is in the situation considered by Schumacher and Westmoreland [15], where initially Alice and Bob are decoupled from Eve, and one can then implement their protocol. That the information that goes through the insecure channel in the first part of the protocol does not leak information to Eve can be seen as follows: Alice locally simulates the symmetric side channel which she would have used to extract mutual independence, and then sends Bob's output to him through the insecure quantum channel and traces out the part that would go to Eve. If Eve intercepts the state, then because of the symmetry of Bob and Eve in the symmetric-side channel, she is just getting the information which would have anyway gotten to her in the case where there was actually a symmetric side channel, and therefore, she has to be decoupled from Alice and Bob's final state.

Finally, Eq. (4) is also interesting in the context of superactivation of the quantum capacity or distillable entanglement. For one thing, it shows that when looking for more superactivation protocols with the symmetric-side channel, one can focus on the rather indiscriminate task of making part of Alice's state product with the environment. In section V we show another connection of superactivation with mutual independence, which relates the weak mutual independence rate *without* assistance by any side channel, with the maximum coherent information (whose regularization gives the distillable entanglement) achievable with the assistance of an erasure channel. This is a channel obtained by a particular encoding of the symmetric-side channel and is the one actually used in all concrete examples of non-additivity found so far [16], [19], [20], [21], [26]. This suggests that weak mutual independence might not be increased by symmetric-side channels, which would be a considerable improvement of Eq. (4), but which we leave as an open problem.

## II. BACKGROUND AND DEFINITIONS

The *symmetric-side channel* is defined by the property that it maps the input state symmetrically to the receiver and the environment. For completeness, and in detail, we follow Ref. [10]: consider the symmetric subspace  $\mathcal{S}_d$  between two  $d$ -dimensional Hilbert spaces spanned by the basis:

$$|(i, j)\rangle := \begin{cases} \frac{1}{\sqrt{2}}(|i, j\rangle + |j, i\rangle) & \text{for } i < j \\ |i, i\rangle & \text{for } i = j. \end{cases} \quad (6)$$

Let  $U_{ss,d} : A \hookrightarrow BE$ , with  $A \cong \mathbb{C}^{d(d+1)/2}$  and  $BE \cong \mathcal{S}_d$ , be an isometry which maps a basis of the  $d(d+1)/2$ -dimensional Hilbert space into the  $|(i, j)\rangle$ , in some order. Then the  $d$ -dimensional symmetric-side channel is defined as

$$\Lambda_{ss,d}(\rho) := \text{tr}_E U_{ss,d} \rho U_{ss,d}^\dagger. \quad (7)$$

In the (fifty-fifty) *erasure channel*, with probability half the quantum information is sent to the receiver intact, while with probability half the information is completely lost to the environment and the receiver gets an error flag. Let  $U_{e,d} : A \hookrightarrow BE$ , with  $A \cong \mathbb{C}^d$  and  $B, E \cong \mathbb{C}^{d+1}$ , be the isometry defined as

$$U_{e,d}|i\rangle = \frac{1}{2}(|i, e\rangle + |e, i\rangle) \quad (8)$$

for all  $i \in \{0, \dots, d-1\}$ , with  $|e\rangle \equiv |d\rangle$ . Then the erasure channel is given by

$$\begin{aligned} \Lambda_{e,d}(\rho) &:= \text{tr}_E U_{e,d} \rho U_{e,d}^\dagger \\ &= \frac{1}{2}\rho + \frac{1}{2}|e\rangle\langle e|. \end{aligned} \quad (9)$$

For a channel  $\Lambda(\rho) := \text{tr}_E(U\rho U^\dagger)$  we define its complementary channel as  $\Lambda^c(\rho) := \text{tr}_B(U\rho U^\dagger)$ . We say  $\Lambda$  is *anti-degradable* if there is another quantum operation  $\mathcal{E}$  such that  $\Lambda = \mathcal{E} \circ \Lambda^c$ , i.e. Eve can simulate the channel from Alice to Bob by applying the operation  $\mathcal{E}$  [23]. Both the symmetric-side channel and the erasure channel are examples of anti-degradable channels and all such channels have zero quantum capacity [23].

Note that one can use a  $(d+1)$ -dimensional symmetric-side channel to simulate a  $d$ -dimensional erasure channel in a very simple way: the sender only have to encode the  $d$ -dimensional input space into the subspace which gets mapped by  $U_d$  to the subspace  $\{|(i, j)\rangle : i \in \{0, \dots, d-1\}, j = d\}$ . In fact this is a particular case of a more general property of the symmetric-side channel, which can be used to simulate any other anti-degradable channel by appropriate encoding and decoding operations.

**Theorem 1.** *For every anti-degradable channel  $\Lambda$  there is an integer  $d$  and quantum operations  $\mathcal{E}$  and  $\mathcal{F}$  such that*

$$\Lambda = \mathcal{E} \circ \Lambda_{ss,d} \circ \mathcal{F}. \quad (10)$$

The proof of the theorem is given in Appendix A.

We now turn to the four main quantities which we will be concerned with: distillable entanglement [6], secret key [6], mutual independence [22], and weak mutual independence. They are all given by the optimization of a certain cost function over a restricted set of operations. Here we are interested in the following classes of operations:

- Local operations (by Alice and Bob), without communication. We denote this class by  $\emptyset$ .
- Local operations and one-way classical communication from Alice to Bob. The class will be denoted by  $\rightarrow$ .
- Local operations and forward communication by (unlimited many uses of) an erasure channel. The class is denoted by  $e$ .

- Local operations and forward communication by (unlimited many uses of) a symmetric-side channel. The class is denoted by *ss*.

In the following let  $\mathcal{C}$  be one of the class of operations defined above.

**Distillable Entanglement:** Given a (mixed) bipartite state  $\psi_{AB}$ , a  $\mathcal{C}$ -protocol for entanglement distillation is formed by a sequence of maps  $\Lambda^{(n)}$  from  $\mathcal{C}$  such that

$$\lim_{n \rightarrow \infty} \|\Lambda^{(n)}(\psi_{AB}^{\otimes n}) - \Phi(M_n)\|_1 = 0, \quad (11)$$

where  $\Phi(M_n)$  is the  $M_n$ -dimensional maximally entangled state given by

$$\Phi(M_n) = \frac{1}{M_n} \sum_{i=0}^{M_n-1} \sum_{j=0}^{M_n-1} |i, i\rangle \langle j, j|. \quad (12)$$

**Definition 2. (distillable entanglement)** Given a state  $\psi_{AB}$  and an entanglement distillation  $\mathcal{C}$ -protocol  $\mathcal{P} = \Lambda^{(n)}$ , define the rate

$$R(\mathcal{P}, \psi_{AB}) := \liminf_{n \rightarrow \infty} \frac{\log M_n}{n}. \quad (13)$$

The  $\mathcal{C}$ -distillable entanglement of  $\psi_{AB}$  is given by

$$D_{\mathcal{C}}(\psi_{AB}) := \sup_{\mathcal{P}} R(\mathcal{P}, \psi_{AB}), \quad (14)$$

**Distillable Secret-Key:** A  $\mathcal{C}$ -protocol for secret-key distillation is a sequence of maps  $\Lambda^{(n)}$  from  $\mathcal{C}$  with the property that

$$\rho_{ABE}^{(n)} := \Lambda^{(n)} \otimes \text{id}_E(\psi_{ABE}^{\otimes n}), \quad (15)$$

with  $|\psi_{ABE}\rangle$  a purification of  $\psi_{AB}$ , is such that

$$\lim_{n \rightarrow \infty} \left\| \rho_{ABE}^{(n)} - \frac{1}{M_n} \sum_{i=0}^{M_n-1} |i, i\rangle \langle i, i| \otimes \rho_E^{(n)} \right\|_1 = 0. \quad (16)$$

**Definition 3. (distillable secret-key)** Given a state  $\psi_{AB}$ , consider a  $\mathcal{C}$ -protocol for key distillation  $\mathcal{P} = \Lambda^{(n)}$  and define the rate

$$R(\mathcal{P}, \psi_{AB}) := \liminf_{n \rightarrow \infty} \frac{\log M_n}{n}. \quad (17)$$

The  $\mathcal{C}$ -distillable secret-key of  $\rho_{AB}$  is given by

$$K_{\mathcal{C}}(\psi_{AB}) := \sup_{\mathcal{P}} R(\mathcal{P}, \psi_{AB}), \quad (18)$$

Note that distillation of secret key via public communication is completely equivalent to distilling a class of states  $\gamma_n$  called *pbits* via local operations and classical communication [17]. The states  $\gamma_n$  are a broader class of states than pure entangled ebits, which allow Alice and Bob to get (almost) perfect classical correlations unknown to an adversary, who has a purifying system of their state.

**Mutual Independence:** Following [22], we call a  $\mathcal{C}$ -protocol for extracting mutual independence from  $\psi_{AB}$  any sequence of maps  $\Lambda^{(n)}$  from the class  $\mathcal{C}$  with the property that

$$\rho_{ABE}^{(n)} := \Lambda^{(n)} \otimes \text{id}_E(\psi_{ABE}^{\otimes n}) \quad (19)$$

is such that

$$\lim_{n \rightarrow \infty} \|\rho_{ABE}^{(n)} - \rho_{AB}^{(n)} \otimes \rho_E^{(n)}\|_1 = 0. \quad (20)$$

**Weak Mutual Independence:** We define a new quantity, which is a weaker notion of mutual independence where we only require Alice to be product with Eve. We call a protocol for extracting weak mutual independence any sequence of maps  $\Lambda^{(n)}$  from  $\mathcal{C}$  such that

$$\lim_{n \rightarrow \infty} \|\rho_{AE}^{(n)} - \rho_A^{(n)} \otimes \rho_E^{(n)}\|_1 = 0. \quad (21)$$

with  $\rho_{ABE}^{(n)}$  defined in Eq. (19) above.

**Definition 4. (mutual independence and weak mutual independence)** Given a state  $\psi_{AB}$ , consider a  $\mathcal{C}$ -protocol for extracting (weak) mutual independence  $\mathcal{P} = \Lambda^{(n)}$ . Define the rate

$$R(\mathcal{P}, \psi_{AB}) := \liminf_{n \rightarrow \infty} \frac{1}{2n} I(A : B)_{\Lambda^{(n)}(\psi_{AB}^{\otimes n})}. \quad (22)$$

Then we define the  $\mathcal{C}$ -mutual independence rate of  $\psi_{AB}$  as

$$I_{\text{ind}, \mathcal{C}}(\psi_{AB}) := \sup_{\mathcal{P}} R(\mathcal{P}, \psi_{AB}), \quad (23)$$

while the  $\mathcal{C}$ -weak mutual independence rate of  $\rho_{AB}$  is defined as

$$W_{\text{ind}, \mathcal{C}}(\psi_{AB}) := \sup_{\mathcal{P}} R(\mathcal{P}, \psi_{AB}), \quad (24)$$

### III. ONE FORMULA FITS ALL

We have seen that mutual independence and its weak variant can be seen as extensions of distillable entanglement, or distillable secret key, to a setting in which the condition that Alice and Bob's systems are perfectly correlated (either quantumly as ebits or classically as pbits [7]) is dropped, and only the privacy condition that Eve's state is factored out is required. In this section we will derive a capacity formula for weak mutual independence. This turns out to be a generalization of both the formula for one-way distillable entanglement and one-way distillable secret-key derived by Devetak and Winter [6].

Consider the following classes of completely positive (CP) maps:

- *RO (rank-one CP maps)*: all maps  $\Lambda$  of the form  $\Lambda(\sigma) = A\sigma A^\dagger$ .
- *QC (quantum-to-classical maps)*: all maps  $\Lambda$  of the form  $\Lambda(\sigma) = \sum_j \text{tr}(A_j \sigma) |j\rangle \langle j|$ , with  $A_j \geq 0$  and  $\sum_j A_j \leq \text{id}$ .
- *CP (general CP maps)*: this is the class formed by all CP maps.

The next theorem shows that (one-way) distillable entanglement, distillable secret key, and weak mutual independence are given by the same quantity optimized over the three classes of operations defined above, respectively.

**Theorem 5.** For a pure state  $|\psi_{ABE}\rangle$  and a class of operations  $\mathcal{C}$  we define

$$G_{\mathcal{C}}(\psi_{AB}) := \max_{\rho \in \mathcal{C}} \frac{1}{2} (I(a : B|\alpha)_\rho - I(a : E|\bar{\alpha})_\rho) \quad (25)$$

with

$$\rho_{aB\alpha E\bar{\alpha}} := \sum_k p_k (\mathcal{E}_k \otimes \text{id}_{BE})(\psi_{ABE}) \otimes |k, k\rangle_{\alpha\bar{\alpha}} \langle k, k|,$$

and the maximization taken over all sets of CP maps  $\{\mathcal{E}_k : A \hookrightarrow a\}_k$  contained in the class  $\mathcal{C}$  and whose elements sum up to a quantum operation  $\mathcal{E} := \sum_k p_k \mathcal{E}_k$ . Let

$$G_{\mathcal{C}}^{\infty}(\psi_{AB}) := \lim_{n \rightarrow \infty} \frac{1}{n} G_{\mathcal{C}}(\psi_{AB}^{\otimes n}). \quad (26)$$

Then

$$D_{\rightarrow}(\psi_{AB}) = G_{RO}^{\infty}(\psi_{AB}), \quad (27)$$

$$K_{\rightarrow}(\psi_{AB}) = 2G_{QC}^{\infty}(\psi_{AB}), \quad (28)$$

and

$$W_{\text{ind}, \rightarrow}(\psi_{AB}) = G_{CP}^{\infty}(\psi_{AB}). \quad (29)$$

*Proof:* Equation (28) follows directly from Ref. [6], while Eq. (27) is a simple rearrangement of the formula found in Ref. [6]. We only have to note that because each  $\psi_{k, ABE} := (\mathcal{E}_k \otimes \text{id}_{BE})(\psi_{ABE})$  is a pure state, it follows that

$$\begin{aligned} & G_{RO}(\psi_{AB}) \\ &= \lim_{n \rightarrow \infty} \sum_k p_k \frac{1}{2} (I(a : B)_{\psi_k} - I(a : E)_{\psi_k}) \\ &= \lim_{n \rightarrow \infty} \sum_k p_k I(a : B)_{\psi_k} \end{aligned} \quad (30)$$

which is Devetak-Winter formula for the one-way distillable entanglement.

So it remains to prove Eq. (29). Let us start showing the achievability of  $G_{CP}(\psi_{AB})$ , which by block coding implies that  $G_{CP}^{\infty}(\psi_{AB})$  is achievable as well. The protocol has three steps. In the first, Alice applies the operation

$$\mathcal{F}(\sigma) = \sum_k p_k \mathcal{E}_k(\sigma) \otimes |k\rangle\langle k|_X, \quad (31)$$

to  $n$  copies of her share of the state, communicates the classical information in the register  $X$  to Bob and Eve and traces out  $X$ , obtaining  $n$  copies of the state

$$\begin{aligned} & \phi_{aB\alpha E\bar{\alpha}} \\ &= \sum_k p_k (\mathcal{E}_k \otimes \text{id}_{BE})(\psi_{ABE}) \otimes |k, k\rangle_{\alpha\bar{\alpha}} \langle k, k|, \end{aligned} \quad (32)$$

where  $\alpha$  and  $\bar{\alpha}$  are held by Bob and Eve, respectively.

In a second step Alice projects her system into its *typical subspace* [24], outputting an error flag when the projection fails and getting the state  $\phi_{aB\alpha E\bar{\alpha}}^n$ .

Finally, Alice splits her  $a_n$  (which labels the system held by Alice) into two registers  $a_{1,n}$  and  $a_{2,n}$  of size

$$\lim_{n \rightarrow \infty} \frac{1}{n} \log |a_{2,n}| = \lim_{n \rightarrow \infty} \frac{1}{2n} I(a : E\bar{\alpha})_{\phi_{aE\bar{\alpha}}} \quad (33)$$

in such a way that

$$\lim_{n \rightarrow \infty} \|\phi_{a_{1,n} E\bar{\alpha}} - \phi_{a_{1,n}} \otimes \phi_{E\bar{\alpha}}\|_1 = 0. \quad (34)$$

That such a splitting always exists is shown in Lemma 6. As Alice's final state is product with Eve's, the protocol extracts weak mutual independence. The rate is given by

$$\begin{aligned} & \lim_{n \rightarrow \infty} \frac{1}{2n} I(a_{1,n} : B)_{\phi} \\ &= \lim_{n \rightarrow \infty} \left( \frac{1}{2n} I(a_{1,n} a_{2,n} : B)_{\phi} - \frac{1}{2n} I(a_{2,n} : B|a_{1,n})_{\phi} \right), \end{aligned} \quad (35)$$

where we used the chain rule. From the bound

$$I(a_{2,n} : B|a_{1,n}) \leq 2 \log(|a_{2,n}|) \quad (36)$$

and Eq. (33) we then get

$$\begin{aligned} & \lim_{n \rightarrow \infty} \frac{1}{2n} I(a_{1,n} : B)_{\phi} \\ & \geq \lim_{n \rightarrow \infty} \left( \frac{1}{2n} I(a : B)_{\phi} - \frac{1}{2n} I(a : E)_{\phi} \right), \end{aligned} \quad (37)$$

which shows that  $W_{\text{ind}, \rightarrow}(\psi_{AB}) \geq G_{CP}(\psi_{AB})$ .

The converse follows almost directly from the definition of  $W_{\text{ind}, \rightarrow}$ . Consider an optimal protocol for extracting weak mutual independence as in Def. (4). The optimal 1-way LOCC operations  $\Lambda^{(n)}$  can be assumed to have the form

$$\Lambda^{(n)}(\sigma) = \sum_k q_{k,n} (\Lambda_{k,n} \otimes \text{id}_{BE})(\sigma) \otimes |k, k\rangle_{\alpha\bar{\alpha}} \langle k, k| \quad (38)$$

for a quantum instrument  $\{q_{k,n}, \Lambda_{k,n}\}$  (i.e. a set of CP maps implemented with probability  $q_{k,n}$ ). This is so because any action of Bob would only decrease his mutual information with Alice. Thus the optimal one-way LOCC protocol for  $W_{\text{ind}, \rightarrow}$  consists of Alice applying an instrument to her system and communicating which CP map was implemented to Bob and Eve. Then

$$\begin{aligned} & W_{\text{ind}, \rightarrow}(\psi_{AB}) \\ &= \liminf_{n \rightarrow \infty} \frac{1}{2n} I(A : B\alpha)_{\Lambda^{(n)}(\psi_{AB}^{\otimes n})} \\ &= \liminf_{n \rightarrow \infty} \frac{1}{2n} \left( I(A : B\alpha)_{\Lambda^{(n)}(\psi_{AB}^{\otimes n})} - I(A : E\alpha)_{\Lambda^{(n)}(\psi_{AB}^{\otimes n})} \right) \\ &\geq G_{CP}^{\infty}(\psi_{AB}), \end{aligned} \quad (39)$$

where the second equality follows from the fact that Alice's state is asymptotically product with Eve's, and the last equality comes from the definition of  $G_{CP}^{\infty}$ . ■

**Remark:** Following the proof of the theorem it is also straightforward to derive a formula for the zero-way weak mutual independence:

$$W_{\text{ind}, \emptyset}(\psi_{AB}) = \lim_{n \rightarrow \infty} \frac{1}{n} W_{\text{ind}, \emptyset}^{(1)}(\psi_{AB}^{\otimes n}) \quad (40)$$

with

$$W_{\text{ind}, \emptyset}^{(1)}(\psi_{AB}) := \max_{A \rightarrow a\alpha} \frac{1}{2} (I(a : B) - I(a : E)), \quad (41)$$

where the maximization is taken over all isometries mapping  $A$  to  $a\alpha$ .

Also along very similar lines to the proof above, we get the following generalization of the theorem: for a channel  $\Lambda$  define the quantity

$$G_{\Lambda}(\psi_{AB}) := \lim_{n \rightarrow \infty} \lim_{m \rightarrow \infty} \frac{G^{(1)}(\Lambda^{\otimes m}, \psi_{AB}^{\otimes n})}{n} \quad (42)$$

with

$$\begin{aligned} & G^{(1)}(\Lambda, \psi_{AB}) \\ &:= \sup_{A \rightarrow a\alpha_1 \alpha_2} \frac{1}{2} [I(a : \Lambda(\alpha_1)B)_{\phi} - I(a : \Lambda^c(\alpha_1)E)_{\phi}] \end{aligned} \quad (43)$$

where  $\Lambda^c$  is the conjugate channel of  $\Lambda$ , the optimization is taken over all isometries mapping  $|\psi\rangle_{ABE}$  to  $|\psi\rangle_{a\alpha_1\alpha_2BE}$ , and the " $\Lambda(\alpha_1)$ " in the formula is a shorthand for the state obtained by applying  $\Lambda$  to the  $\alpha_1$  register of  $|\phi\rangle_{a\alpha_1\alpha_2BE}$ . Then the distillable entanglement, secret-key capacity, and weak mutual independence capacity (zero-way, one-way, assisted by erasure channel, by a symmetric-side channel, or by any other channel) are all specific cases of this formula for particular choices of the channel  $\Lambda$ .

The following Lemma is proved in [25]:

**Lemma 6.** ([25] *Decoupling Lemma*) *For every bipartite state  $\psi_{AE}$  let  $\psi_{A^n E^n}$  be defined as*

$$|\psi_{A^n E^n}\rangle := P_{n,\varepsilon_n} |\psi_{AE}\rangle^{\otimes n} / \|P_{n,\varepsilon_n} |\psi_{AE}\rangle^{\otimes n}\|, \quad (44)$$

with  $P_{n,\varepsilon_n}$  the projector onto the  $\varepsilon_n$ -typical subspace of  $|\psi_{AE}\rangle^{\otimes n}$ . Then for every sequence  $\{\varepsilon_n\}$  going to zero, there is a sequence of isometries  $V_n : A_n \hookrightarrow A_{1,n} A_{2,n}$  such that

$$\lim_{n \rightarrow \infty} \|\text{tr}_{A_{1,n}} (V_n \psi_{AE}^{\otimes n} V_n^\dagger) - \tau_n \otimes \psi_E^{\otimes n}\|_1 = 0, \quad (45)$$

with  $\tau_n$  the maximally mixed state in  $A_{2,n}$ , and

$$\lim_{n \rightarrow \infty} \frac{\log |A_{1,n}|}{n} = I(A : E)_\psi \quad (46)$$

#### IV. ASSISTED CAPACITIES ARE EQUAL

In this section we prove that under the assistance of an erasure channel or a symmetric-side channel, distillable entanglement, mutual independence, and weak-mutual independence become the same. This result is used in Ref. [11] to show that these symmetric-side channel assisted capacities give the optimal rate at which a quantum state shared by Alice and Bob can be used as a one-time-pad to encrypt quantum messages which are sent down an insecure quantum channel.

In the following lemma we give a characterization of states with perfect weak mutual independence analogous to the characterization of [17] for pbits and of [22] for states with perfect mutual independence. We say a state  $|\psi_{a\alpha BE}\rangle$  has perfect weak mutual independence if  $\psi_{aE} = \psi_a \otimes \psi_E$ .

**Lemma 7.** *A state  $|\psi_{a\alpha BE}\rangle$  has perfect weak mutual independence if, and only if, there is an isometry  $U : \alpha B \rightarrow \bar{a}\bar{E}$  such that*

$$U|\psi_{a\alpha BE}\rangle = |\phi_{a\bar{a}}\rangle \otimes |\chi_{e\bar{e}}\rangle \quad (47)$$

*Proof:* It is clear that any state satisfying Eq. (47) has perfect weak mutual independence. To show the converse, we note that if  $\psi_{aE} = \psi_a \otimes \psi_E$ , there is a purification of  $\psi_{aE}$  of the form  $|\phi_{a\bar{a}}\rangle \otimes |\chi_{e\bar{e}}\rangle$ . But as  $|\psi_{a\alpha BE}\rangle$  is another purification of  $\psi_{aE}$ , by Uhlmann's theorem these two states must be related by an isometry acting on the purifying subsystem  $\alpha B$ . ■

In [26] an intuitive explanation and generalised protocol for Smith and Yard's examples of superactivation [16] was presented. Given a pbit, one can use the erasure channel to send Alice's part of the *shield* [17] to Bob. This process then generates a state with coherent information equals half the size of the *key* part of the pbit. Then, by considering the process in which Alice and Bob first distill pbits from their state and

then use the erasure channel to convert them into distillable entanglement, we get Eq. (3).

A very similar protocol works also for mutual independence and weak mutual independence. For the latter, the  $\alpha B$  register can be seen as the shield part of the state, which protects  $\psi_a$  from having correlations with  $\psi_E$ . The amount of key is given by half the mutual information of the  $a$  and  $B$  registers. Now suppose Alice sends her share of the shield  $\alpha$  through an erasure channel to Bob. With probability half, Bob gets  $\alpha$ . Then he can apply the isometry  $U$  of Lemma 7, getting  $S(a)$  of coherent information with Bob. In the case where Bob receives the erasure flag, they will end up with a state with coherent information  $I(a)B$ . Because Bob knows which case happened, the total coherent information is given by the average of the two, which is just the weak mutual independence of  $\psi_{a\alpha B}$ ,  $I(a : B)/2$ . More formally, we have

**Theorem 8.** *For a bipartite state  $\psi_{AB}$ ,*

$$W_{\text{ind},E}(\psi_{AB}) = I_{\text{ind},E}(\psi_{AB}) = D_E(\psi_{AB}) \quad (48)$$

and, likewise,

$$W_{\text{ind},ss}(\psi_{AB}) = I_{\text{ind},ss}(\psi_{AB}) = D_{ss}(\psi_{AB}). \quad (49)$$

*Proof:* It is clear that  $W_{\text{ind},E}(\psi_{AB}) \geq I_{\text{ind},E}(\psi_{AB}) \geq D_E(\psi_{AB})$ . So let us show

$$D_E(\psi_{AB}) \geq W_{\text{ind},E}(\psi_{AB}). \quad (50)$$

Consider the optimal protocol for  $W_{\text{ind},E}(\psi_{AB})$ . We can assume all the classical communication is made by using the erasure channel and that no system is discarded until the very end. In the final step the state shared by Alice, Bob and Eve is  $|\phi_{a\alpha:B:E}^n\rangle$ , with the property that

$$\lim_{n \rightarrow \infty} \|\phi_{a:E}^n - \phi_a^n \otimes \phi_E^n\|_1 = 0, \quad (51)$$

and

$$W_{\text{ind},E}(\psi_{AB}) = \liminf_{n \rightarrow \infty} \frac{1}{2n} I(a : B)_{\phi_{a\alpha:B:E}^n}. \quad (52)$$

Now, suppose that Alice instead of discarding  $\alpha$ , sends it down the erasure channel. Then the global state becomes

$$\frac{1}{\sqrt{2}} |\phi_{a:B\alpha:E}^n\rangle \otimes |e\rangle_{E'} + \frac{1}{\sqrt{2}} |\phi_{a:B:E\alpha}^n\rangle \otimes |e\rangle_{B'}. \quad (53)$$

Due to the orthogonality of the erasure flag to the rest of the state, the coherent information of Alice's and Bob's subsystems splits into two as

$$\frac{1}{2} I(a)B + \frac{1}{2} I(a)B\alpha = \frac{1}{2} I(a)B - \frac{1}{2} I(a)E \quad (54)$$

where we used the identity  $I(X)Y = -I(X)Z$ , valid for all pure states  $|\phi\rangle_{XYZ}$ . Then, by the hashing inequality [6],

$$\begin{aligned} D_E(\psi_{AB}) &\geq \lim_{n \rightarrow \infty} \frac{1}{2} I(a)B - \frac{1}{2} I(a)E \\ &= \lim_{n \rightarrow \infty} \frac{1}{2} I(a)B + \frac{1}{2} S(a) \\ &= \lim_{n \rightarrow \infty} \frac{1}{2} I(a : B) \\ &= W_{\text{ind},E}(\psi_{AB}), \end{aligned} \quad (55)$$



where the before-last equality follows from the fact that  $a$  and  $E$  are asymptotically product (see Eq. 51).

The proof for the ss-assisted quantities is completely analogous. We only have to use the observation made in section II that a symmetric-side channel can be used to simulate an erasure channel and apply the reasoning from before. ■

**Remark 1:** We note that we do not know whether the ss-assisted distillable secret-key is equal to the other quantities, and we conjectured that it is not. Indeed, for an EPR pair all the quantities are equal to one. For a pbit [7], in turn, the distillable secret-key is equal to one, while we only have the Smith-Yard bound  $D_{ss}(\psi_{AB}) \geq K_{ss}(\psi_{AB})/2$  [16], which we expect to be tight when the shield part of the pbit is composed of a separable state.

**Remark 2:** The theorem can be applied to any channel for which sending the shield part of a state with perfect weak mutual independence does not decrease the weak mutual independence rate (which is the case for the symmetric-side channel and the erasure channel): for any such channel  $\Lambda$ , we have  $W_\Lambda = D_\Lambda$ .

## V. SUPERACTIVATION AND WEAK MUTUAL INDEPENDENCE

In this section we show that weak mutual independence is related to how much the erasure channel can activate the distillable entanglement of a given state, at least under a restricted class of protocols. Let  $D_E^{(1)}(\psi_{AB})$  be the maximum coherent information assisted by an erasure channel, defined as

$$D_E^{(1)}(\psi_{AB}) := \max_{A \hookrightarrow a\alpha} I(a)BB')_{\omega_{aBB'}} \quad (56)$$

with  $\omega_{aBB} := \Lambda_E(\psi_{a\alpha B})$  and  $\Lambda_E : \alpha \hookrightarrow b$  an erasure channel, and where the maximization is taken over all isometric splittings of  $A$  into  $a\alpha$ . We can fully characterize this quantity by weak mutual independence rate as follows.

**Proposition 9.**

$$\begin{aligned} D_E^{(1)}(\psi_{AB}) &= W_{ind,\emptyset}^{(1)}(\psi_{AB}) \\ &= \max_{A \hookrightarrow a\alpha} \frac{1}{2} (I(a : B) - I(a : E)). \end{aligned} \quad (57)$$

*Proof:* A simple calculation gives

$$D_E^{(1)}(\psi_{AB}) = \max_{A \hookrightarrow a\alpha} \frac{1}{2} I(a)B\alpha)_{\psi_{a\alpha B}} + \frac{1}{2} I(a)B)_{\psi_{a\alpha B}}. \quad (58)$$

Writing the purification of  $\psi_{a\alpha B}$  as  $\psi_{a\alpha BE}$  we then find

$$\begin{aligned} D_E^{(1)}(\Psi_{AB}) &= \max_{A \hookrightarrow a\alpha} \frac{1}{2} I(a)B\alpha)_{\psi} + \frac{1}{2} I(a)B)_{\psi} \\ &= \max_{A \hookrightarrow a\alpha} \frac{1}{2} I(a)B\alpha)_{\psi} - \frac{1}{2} I(a)E\alpha)_{\psi} \\ &= \max_{A \hookrightarrow a\alpha} \frac{1}{2} I(a)B)_{\psi} - \frac{1}{2} I(a)E)_{\psi}. \end{aligned} \quad (59)$$

A corollary of the theorem is that there are states for which  $W_{ind,\emptyset}(\psi_{AB}) \gg K_{\rightarrow}(\psi_{AB})$ . An example is given by the

Jamiołkowski state  $\psi_{AB}$  of the *rocket channel* of [21], where it was shown that  $D_E^{(1)}(\psi_{AB}) \gg K_{\rightarrow}(\psi_{AB})$  (with the difference being of order of the number of qubits of Alice's state).

By the same reasoning we also get that there are states for which the entanglement measure *squashed entanglement* ( $E_{sq}$ ) [27] is much larger than the one-way distillable secret key. This comes from the observation that the squashed entanglement is an upper bound on  $W_{ind,\emptyset}$  (a fact proven implicitly in [25] and explicitly in [22]) and so for the state associated with the rocket channel,

$$E_{sq}(\psi_{AB}) \geq W_{ind,\emptyset}(\psi_{AB}) = D_E^{(1)}(\psi_{AB}) \gg K_{\rightarrow}(\psi_{AB}). \quad (60)$$

Since the entanglement of formation  $E_f$  can be much greater than the squashed entanglement [28], we also have that  $E_f \gg W_{ind}$  is possible.

## VI. CONCLUSIONS

The capacity of a quantum channel is difficult to calculate because the best formula we have [29], [30], [31], the coherent information, requires an optimisation over an arbitrarily large number of usages of the channel. The symmetric side-channel was originally introduced to provide some insight into this optimisation – it gives a more tractable upper-bound on the capacity of a channel, since when used in conjunction with any channel, the combined capacity is single-letter.

However, here, and in [11], we have seen that the symmetric-side channel is more than a calculational tool. It should be thought of as playing the role of public quantum communication, in the same way as public classical communication makes the theory of private classical channels more elegant and physically natural. The symmetric side-channel is conceptually analogous to what one demands of a notion of public quantum communication (the receiver and eavesdropper both get the same information), and it furthermore makes the rates for distilling entanglement equivalent in form to the rates of distilling private key using public classical communication.

The similarity between entanglement and private correlations was used in constructing the first entanglement distillation protocols, and has been used to conjecture new types of classical distributions [32]. But the analogy between privacy and entanglement was first made fully explicit by Collins and Popescu [33] and extended in [34]. The identification of the symmetric side-channel with public classical communication completes this analogy.

We have seen that the introduction of public quantum communication makes the rate for distilling entanglement have a similar form as the rate for distilling classical key. Likewise, it allows for correcting noisy correlations, in much the same way as in the classical case. This gives further motivation for the study of mutual independence, and the weak mutual independence introduced here. It also helps us understand the phenomena of superactivation, and more generally, non-additivity of the channel capacity: the symmetric side-channel has no capacity, but it helps correct errors introduced by a noisy quantum channel, in much the same way that classical communication allows for error reconciliation of private correlations. A better understanding of weak mutual independence



thus provides a way to better understand superactivation and other forms of non-additivity.

The mutual independence and the weak mutual independence also help us understand tripartite correlations. It quantifies how two parties can be correlated (or decoupled) from a third party. Mutual independence quantifies how hard it is for the global state to be decoupled while still retaining bipartite correlations, while the weak mutual independence quantifies how hard it is for one party to decouple. To quantify how hard it is for each party to individually decouple from the third party (while retaining bipartite correlations), one can consider the *not-so-weak mutual independence*, where we demand individual privacy but not collective privacy:  $\rho_{AE} \simeq \rho_A \otimes \rho_E$  and  $\rho_{BE} \simeq \rho_B \otimes \rho_E$ . How this compares to the original mutual independence, enables one to quantify the extent to which a third party is *correlated to the correlations* of two parties. It thus enables a better understanding of genuine tripartite correlations, a concept which is not well characterised even in the classical case. This is reminiscent of attempts to understand bipartite correlations (and mutual information) in terms of the number of unitaries needed to decouple a state from another [35].

The work here raises a lot of open questions. For example, we do not even know if the erasure channel or the symmetric side-channel helps in distilling weak mutual independence. For that matter, it is possible that even a classical communication channel is not helpful. It is possible, that these additional channels are only useful for correcting errors (i.e. turning mutual independence into EPR pairs). It is also possible that the erasure channel is as good as the symmetric-side channel for distilling weak mutual-independence, and hence for superactivation of private states. Indeed, for general private states, the erasure channel appears to provide the optimal protocol [26]. Using the results of Section II it would then be the optimal anti-degradable channel.

This work also suggests several questions about categories of states and channels. Are there states which have weak mutual independence, but from which no private key can be distilled? This is related to the problem of *bound key* [32]. Can we find a characterization of the convex set of states with zero  $D_{ss}$ ? Can we characterize the class of channels which have zero capacity for generating weak mutual independence? Can we use the connection between mutual independence and channel capacity to find more examples of non-additivity and superactivation?

Finally, although Eq. (2) is single-letter, it is of little practical use, as it involves an optimization over a system of unbounded dimension. Can we upper bound the size of the register that goes in the symmetric-side channel in the optimal protocol, in analogy to what can be done in the classical case?

#### ACKNOWLEDGEMENTS

We are grateful to Graeme Smith for interesting discussions, and his helpful comments on an early draft of this work. JO thanks the hospitality of KITP, Santa Barbara during his stay.

#### APPENDIX

##### Proof of Theorem 1

Let  $U_\Lambda : A \hookrightarrow BE$  be an isometric extension of  $\Lambda$ . Since  $\Lambda$  is anti-degradable, there is an isometry  $V : E \hookrightarrow FG$  such that

$$|\phi\rangle_{RBF G} := (V^{E \rightarrow FG} \circ U_\Lambda^{A \rightarrow BE}) |\psi\rangle_{RA} \quad (61)$$

have equal  $RB$  and  $RF$  reduced states (i.e.  $\phi_{RB} = \phi_{RF}$ ) for every state  $|\psi_{RA}\rangle$ , where  $R$  is a reference system.

Define the state

$$\begin{aligned} |\Psi\rangle_{RBF G_1 G_2 H_1 H_2} &:= \frac{1}{\sqrt{2}} U_{ss,|G|}^{G \rightarrow G_1 G_2} |\phi\rangle_{RBF G} \otimes |00\rangle_{H_1 H_2} \\ &+ \frac{1}{\sqrt{2}} \text{SWAP}_{BF} \left( U_{ss,|G|}^{G \rightarrow G_1 G_2} |\phi\rangle_{RBF G} \right) \otimes |11\rangle_{H_1 H_2}, \end{aligned}$$

with  $\text{SWAP}_{BF}$  the unitary which swaps subsystems  $B$  and  $F$ . By construction  $\Psi_{RB} = \frac{1}{2}(\phi_{RB} + \phi_{RF}) = \phi_{RB}$  and so the states  $|\Psi\rangle$  and  $|\phi\rangle$  are related by an isometry from  $FG$  to  $FG_1 G_2 H_1 H_2$ . Therefore it suffices to show how Alice and Bob can create the state  $|\Psi\rangle$  (with Eve holding the  $FG_1 G_2 H_1 H_2$  registers) by a symmetric-side channel and local operations.

Note that  $|\Psi\rangle$  is permutation symmetric with respect to the subsystems  $\alpha := BG_1 H_1$  and  $\bar{\alpha} := FG_2 H_2$ . Thus there is a pre-image state  $|\Phi\rangle_{RS}$  such that

$$|\Psi\rangle_{RBF G_1 G_2 H_1 H_2} = U_{ss,|S|}^{S \rightarrow \alpha \bar{\alpha}} |\Phi\rangle_{RS}. \quad (62)$$

Alice and Bob's protocol is the following: Alice transforms  $|\psi_{RA}\rangle$  into  $|\Phi\rangle_{RS}$  by applying an operation  $\mathcal{E} : A \rightarrow S$  (which always exists because  $\psi_R = \Phi_R$ ). Then she sends  $S$  through a symmetric-side channel producing the state  $|\Psi\rangle$ , where Alice and Eve hold the  $BG_1 H_1$  and  $FG_2 H_2$  registers, respectively. Finally, Bob applies his local operation  $\mathcal{F}$  which consists of tracing out the register  $G_1 H_1$ .

#### REFERENCES

- [1] U.M. Maurer. Secret Key Agreement by Public Discussion from Common Information. IEEE Trans. Info. Theory **39**, 733 (1993).
- [2] R. Ahlswede and I. Csiszar. Common Randomness in Information Theory and Cryptography Part II. IEEE Trans. Inf. Theory **39**, 1121 (1993).
- [3] I. Csiszar and J. Korner. Broadcast Channels with Confidential Messages. IEEE Trans. Inf. Theory **24**, 339 (1978).
- [4] A. D. Wyner. The wire-tap channel. Bell Sys. Tech. J. **54**, 1355 (1975).
- [5] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki. Quantum Entanglement. Rev. Mod. Phys. Vol. 81, No. 2, pp. 865-942 (2009).
- [6] I. Devetak and A. Winter. Distillation of secret key and entanglement from quantum states. Proc. R. Soc. Lond. A **461**, 207 (2005).
- [7] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim. General paradigm for distilling classical key from quantum states. IEEE Trans. Inf. Theory **55**, 1898 (2009).
- [8] W.K. Wootters and W.H. Zurek. A Single Quantum Cannot be Cloned. Nature **299**, 802 (1982).
- [9] D. Dieks. Communication by EPR devices. Physics Letters A **92**, 271 (1982).
- [10] G. Smith, J.A. Smolin, A. Winter. The quantum capacity with symmetric side channels. IEEE Trans. Info. Theory **54**, 9, 4208 (2008).
- [11] F.G.S.L. Brandão and J. Oppenheim. The quantum one-time pad in the presence of an eavesdropper. arXiv:1004.3328.
- [12] P.O. Boykin and V. Roychowdhury. Optimal encryption of quantum bits. Phys. Rev. A **67**, 042317 (2003).
- [13] A. Ambainis, M. Mosca, A. Tapp, R. de Wolf. Private quantum channels. Proc. IEEE Conf. on Found. Comp. Sci. (FOCS), 2000.
- [14] D.W. Leung. Quantum Vernam Cipher. quant-ph/0012077.
- [15] B. Schumacher and M.D. Westmoreland. Quantum mutual information and the one-time pad. Phys. Rev. A **74**, 042305 (2006).
- [16] G. Smith and J. Yard. Quantum Communication With Zero-Capacity Channels. Science **321**, 1812 (2008).

- [17] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim. Secure key from bound entanglement. *Phys. Rev. Lett.* **94**, 160502 (2005).
- [18] K. Horodecki, L. Pankowski, M. Horodecki, and P. Horodecki. Low dimensional bound entanglement with one-way distillable cryptographic key. *IEEE Trans. Inf. Theory* **54**, 2621 (2008).
- [19] G. Smith and J.A. Smolin. Can non-private channels transmit quantum information? *Phys. Rev. Lett.* **102**, 010501 (2009).
- [20] K. Li, A. Winter, X. Zou, and G. Guo. The private capacity of quantum channels is not additive. *Phys. Rev. Lett.* **103**, 120501 (2009).
- [21] G. Smith and J.A. Smolin. Extensive nonadditivity of privacy. *Phys. Rev. Lett.* **103**, 120503 (2009).
- [22] M. Horodecki, J. Oppenheim, A. Winter. Quantum Mutual Independence. *arXiv:0902.0912v2 [quant-ph]*.
- [23] I. Devetak and P.W. Shor. The capacity of a quantum channel for simultaneous transmission of classical and quantum information. *Comm. Math. Phys.* **256**, 287 (2005).
- [24] B. Schumacher. Quantum Coding. *Phys. Rev. A* **51**, 2738 (1995).
- [25] A. Abeyesinghe, I. Devetak, P. Hayden, A. Winter. The Mother of all Protocols: Reconstructing Quantum Information's Family Tree. *arXiv:quant-ph/0606255*.
- [26] J. Oppenheim. For quantum information, two wrongs can make a right. *Science* **321**, 1783 (2008).
- [27] M. Christandl and A. Winter. "Squashed Entanglement" - An Additive Entanglement Measure. *J. Math. Phys.* **45**, 829 (2004).
- [28] M. Christandl and A. Winter. Uncertainty, Monogamy, and Locking of Quantum Correlations. *IEEE Trans. Inf. Theory* **51**, 3159 (2005).
- [29] S. Lloyd. Capacity of the noisy quantum channel. *Phys. Rev. A* **55**, 1613 (1997).
- [30] P.W. Shor. The quantum capacity and coherent information. Unpublished lecture notes. Online at <http://www.msri.org/publications/ln/msri/2002/quantumcrypto/shor/1>; MSRI Quantum Information, Berkeley, 2002.
- [31] I. Devetak. The private quantum capacity and Quantum Capacity of a Quantum Channel. *IEEE Trans. Info. Theory* **51**, 44 (2005).
- [32] N. Gisin and S. Wolf. Linking Classical and Quantum Key Agreement: Is There "Bound Information"? *Proceedings of CRYPTO 2000, Lecture Notes in Computer Science* **1880**, 482 (2000).
- [33] D. Collins and S. Popescu. A classical analogue of entanglement. *Phys. Rev. A* **65**, 032321 (2002).
- [34] J. Oppenheim, R.W. Spekkens and A. Winter. A classical analogue of negative information. *arXiv:quant-ph/0511247*.
- [35] B. Groisman, S. Popescu and A. Winter. On the quantum, classical and total amount of correlations in a quantum state. *Phys. Rev. A* **72**, 032317 (2005).